

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of

**Rules and Regulations Implementing the
Controlling the Assault of Non-Solicited
Pornography and Marketing Act of 2003**

)
)
)
)
)

CG Docket No. 04-53

COMMENTS OF VERIZON WIRELESS

VERIZON WIRELESS

John T. Scott, III
Charon Phillips
1300 I Street, N.W.
Suite 400 West
Washington, D.C. 20005
(202) 589-3740

April 30, 2004

Its Attorneys

SUMMARY

Verizon Wireless supports a strong national policy against spam. To implement the *CAN-SPAM Act* and impede the proliferation of spam, the FCC must require senders of mobile service commercial messages other than wireless carriers to obtain express prior authorization before sending a message to a mobile device. Opt-in consent should be obtained in a clear, easily understandable form. The Commission should also find that senders may only take advantage of the exemption from opt-in consent for transactional or relationship messages where the sender has an established business relationship with the recipient, and that messages forwarded to mobile devices are not subject to the regulations governing mobile service messages.

Wireless carriers like Verizon Wireless are, however, in a unique relationship with their subscribers. Subscribers elect to be served by their carriers. The *CAN-SPAM Act* therefore authorizes the Commission to exempt a customer's own carrier from the express prior authorization requirement, and the Commission should do so. Particularly given the constitutional infirmities inherent in restricting a carrier's communications to its own customers, the Commission should exempt wireless carriers from the express prior authorization requirement, but only where the wireless carrier does not charge its customers for receiving mobile service commercial messages.

Finally, the Commission should not require wireless carriers to adopt specific technical solutions for permitting electronic disapproval of commercial messages given that the duty to comply with the electronic disapproval requirement rests solely on the party sending mobile service commercial messages.

TABLE OF CONTENTS

BACKGROUND	1
I. THE COMMISSION SHOULD ADOPT STRINGENT MEASURES AGAINST SPAM	5
A. Each Sender of MSCMs Must Obtain Express Prior Authorization Before Initiating a Message to a Mobile Device	6
B. Senders of MSCMs Must Seek Consent in Clear, Easily Understandable Form.....	7
II. MSCMs DO NOT INCLUDE TRANSACTIONAL, RELATIONSHIP, OR FORWARDED MESSAGES.....	7
A. Transactional and Relationship Messages Require an Established Business Relationship.....	8
B. Forwarded Messages Should Not Be Subject to the Restrictions That Apply to MSCMs.....	11
III. THE COMMISSION SHOULD EXEMPT WIRELESS CARRIERS FROM THE REQUIREMENT TO SEEK EXPRESS PRIOR AUTHORIZATION.....	11
A. Wireless Carriers Are in a Unique Position With Their Subscribers.....	12
B. Opt-in Consent is Disfavored Under The First Amendment	14
IV. THE COMMISSION SHOULD NOT CREATE A NATIONAL “DO-NOT-SMS” REGISTRY	16
V. THE FCC SHOULD AVOID MANDATING SPECIFIC TECHNICAL SOLUTIONS FOR PREVENTING SPAM	17
CONCLUSION.....	19

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Rules and Regulations Implementing the)	CG Docket No. 04-53
Controlling the Assault of Non-Solicited)	
Pornography and Marketing Act of 2003)	

COMMENTS OF VERIZON WIRELESS

Verizon Wireless respectfully submits comments on the *Notice*¹ in the captioned proceeding. Verizon Wireless urges the Commission to adopt stringent new prohibitions against spam while allowing wireless carriers to continue to communicate with their customers as long as they do not charge for commercial messages.

BACKGROUND

The legislative history of the *CAN-SPAM Act*² aptly states that “[a]s cumbersome and annoying as spam to a desktop computer is, at least a consumer can turn off their computer and walk away. Wireless spam is even more intrusive because spam to wireless phones is the kind of spam that follows you wherever you go and according to U.S. wireless carriers, is already on the rise.”³ Spam is not just a problem for individual customers, who in addition to the annoyance of receiving spam are often paying for it on

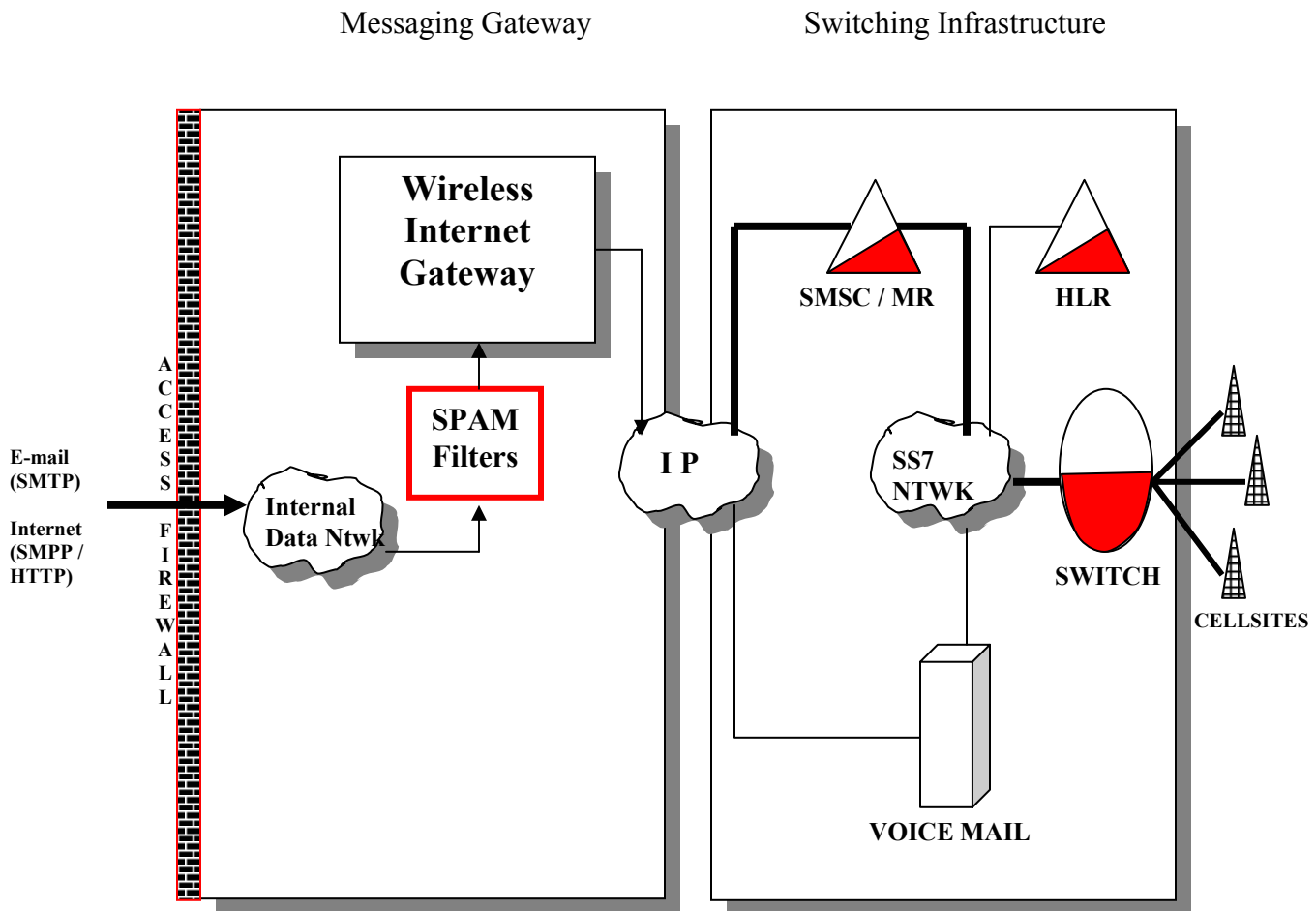
¹ Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, *Notice of Proposed Rulemaking and Further Notice of Proposed Rulemaking*, CG Docket No. 04-53, CG Docket No. 02-278 (rel. Mar. 19, 2004) (“*Notice*”).

² Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003), *codified at* 15 U.S.C. § 7701 (“*CAN-SPAM Act*”).

³ 149 Cong. Rec. H12193-7, H12195 (daily ed. Nov. 21, 2003) (statement of Rep. Markey) (“*Markey Statement*”).

a per-message basis. Spam can also overwhelm and even bring down networks, causing major outages and degradation of network performance. Verizon Wireless therefore supports a strong national policy against spam.

Today customers receive most of their mobile messages through the Verizon Wireless Short Messaging Service (“SMS”), which delivers 160 character text messages to subscribers on the Verizon Wireless digital network. Most spam reaches Verizon Wireless customers through a “gateway” that receives messages from the Internet. The gateway processes messages and directs them to the proper switching elements for delivery to the subscriber. This gateway is commonly referred to as the Wireless Internet Gateway (“WIG”). It receives all public, Internet-based e-mail, Short Message Transfer Protocol (“SMTP”), HyperText Markup Language (“HTML”), and machine-to-machine messaging input enabling desktop access to the Verizon Wireless messaging network. The WIG also serves as the platform for operating the Verizon Wireless “vtext” messaging service and “single sign-on” point of access platform for subscriber access to and management of other messaging platforms including alerts, communities chat, and instant messaging services and subscriber-level spam controls, calendars, and other personalization options. The following figure depicts the SMS network architecture.



Verizon Wireless has deployed spam protections at several levels that are designed to protect Verizon Wireless subscribers from unsolicited commercial messages. Spam generators send the Verizon Wireless network over ten million unsolicited commercial messages each month. Verizon Wireless maintains three layers of protection against such spam: (1) an access firewall, (2) spam filters, and (3) subscriber safeguards.

The Verizon Wireless access firewall protects the Verizon Wireless network from direct access “hacking” by outside parties. Once inside the firewall, spam filter hardware and software further limit messaging throughput to the Verizon Wireless network infrastructure through use of automatic volume, source, and content filters. Volume filters limit messages based on the number allowed per hour, after which messages are

erased. The problem with volume filters, however, is that sometimes spammers “tumble” addresses to bypass spam filters. “Tumbling” is the process of varying the address from which the spam is originating so that it appears to come from a different source. Source filters add another layer of protection by blocking specific known spam offenders from sending any messages through the network. Content filters are more complicated because they examine subject and content fields for keywords or indicators for spam message content, and if a message contains such content, then the messages are erased. The content filters used by Verizon Wireless can look at up to 90 characteristics of a message to help determine whether the message is spam.

Finally, in the last steps before a message reaches a Verizon Wireless subscriber, it passes through gateway filters and subscriber-managed tools that combat spam. Gateways examine source identities after the principal filter elements pass the messages and provide further protection against “tumbling” and “spoofed”⁴ identities from passing spam into the network. Registered subscribers can also block (1) all e-mail sources, (2) all Internet sources; (3) specific e-mail source addresses; and/or (4) specific domain source addresses.

Although these current methods for protecting against spam have begun to impede the flow of spam to Verizon Wireless subscribers, Verizon Wireless is in the process of engineering further protections against spam that will provide subscribers with even greater individual control over the receipt of spam. These include additional filtering that will allow subscribers to establish permission and blocking lists for message sources related to all of the data services offered by Verizon Wireless, and greater

⁴ Spoofing is the practice of “stealing” legitimate e-mail addresses and masking the sender’s identity by using those addresses as source addresses for spam messages.

heuristic spam identification technologies, which should result in greater success in content and source identification for spam content.

In addition to the internal network and subscriber measures that Verizon Wireless has undertaken to battle spam, Verizon Wireless has pursued litigation against the most egregious spammers. For instance, Verizon Wireless filed civil suits against a national mortgage lender in Denver and a telemarketing company in Phoenix, as well as certain "John Doe" defendants responsible for disabling a Verizon Wireless SMS router and transmitting particularly offensive and vulgar messages to our customers. We ultimately identified the John Doe defendants after issuing subpoenas to the Internet service providers through which the messages passed. In each of these cases, Verizon Wireless entered settlement agreements pursuant to which the spammers agreed to cease and desist from sending any further spam messages to Verizon Wireless customers, among other relief. These lawsuits are extremely costly, however, which underscores the need for stringent protections against spam.

Given the critical need for a nationwide policy on spam, the *CAN-SPAM Act* is a timely and positive development. The Commission should adopt stringent protections against unwanted mobile service commercial messages ("MSCMs"), while at the same time allowing wireless carriers to continue to communicate with their customers as long as they do not charge for commercial messages.

I. THE COMMISSION SHOULD ADOPT STRINGENT MEASURES AGAINST SPAM

Congress recognized that spam sent to mobile devices is a rapidly developing problem all over the world. For instance, the legislative history of the *CAN-SPAM Act*

notes that “[i]n Japan alone, NTT DoCoMo estimates that its wireless network processes some 800 million wireless spam messages a day. That is a day.”⁵

To deal with this phenomenon, the *CAN-SPAM Act* requires the Commission to adopt rules that provide wireless subscribers with the ability to avoid receiving MSCMs unless the subscribers have granted the sender of the MSCM “express prior authorization.”⁶ Under the *CAN-SPAM Act*, “express prior authorization” means “opt-in” consent.⁷ The Commission should adopt stringent rules detailing how senders of MSCMs must obtain opt-in consent.

A. Each Sender of MSCMs Must Obtain Express Prior Authorization Before Initiating a Message to a Mobile Device

The legislative history of the *CAN-SPAM Act* makes clear that each entity seeking to send MSCMs must obtain “express prior authorization” before sending MSCMs to mobile devices.⁸ The Commission should clarify that this means that blanket authorization will not suffice.

Senders of MSCMs should not be permitted to seek authorization to send MSCMs by generating SMS messages. Express prior authorization, whether provided in writing or electronically, should occur before a company can send a wireless customer any SMS

⁵ *Markey Statement* at H12193.

⁶ *CAN-SPAM Act*, §14(b)(1).

⁷ *Markey Statement* at H12195-6 (“The wireless spam provision of the bill offers wireless consumers relief by requiring an “opt-in” for spam to wireless consumers. This reflects the fact that spam to a mobile phone is more intrusive to consumers and the fact that some wireless payment plans currently charge users for the amount of text messages they receive.”)

⁸ *Id.* (“[E]ach entity seeking to send mobile service commercial messages pursuant to Section 14(b)(1) [must] obtain such consumer authorization.”) However, the law authorizes the FCC to exempt wireless carriers from this requirement.

messages. Given that customers often pay on a per-message basis for SMS, the Commission should not permit companies to seek consent by sending an SMS message.

As further discussed below, the *CAN-SPAM Act* permits parties to generate “transactional and relationship” messages without consent.⁹ An SMS message sent for the purpose of requesting approval to send MSCMs would not be a “transactional or relationship” message, particularly in the case where the customer had no prior business relationship with the company. Section 3(17), which defines “transactional or relationship” messages, clearly contemplates a prior business relationship between the sender and recipient of the transactional or relationship message. The Commission should therefore prohibit such “cold” messaging.

B. Senders of MSCMs Must Seek Consent in Clear, Easily Understandable Form

In adopting the *CAN-SPAM Act*, Congress expressed its intent for “express prior authorization” to be obtained such that it is “conspicuous and easily understood” by consumers.¹⁰ Although the Commission need not mandate the specific form of the consent that parties seeking to send MSCMs should follow, the Commission’s customer proprietary network information (“CPNI”) rules contain guidelines on seeking consent that might be useful in this context.¹¹

II. MSCMs DO NOT INCLUDE TRANSACTIONAL, RELATIONSHIP, OR FORWARDED MESSAGES

Express prior authorization is only necessary to send MSCMs. The *CAN-SPAM Act* defines an MSCM as “a commercial electronic mail message that is transmitted

⁹ *CAN-SPAM Act*, § 3(17).

¹⁰ *Markey Statement* at H12196.

¹¹ 47 C.F.R. § 64.2008(c).

directly to a wireless device that is utilized by a subscriber of...[CMRS]...in connection with that service.”¹² The Commission seeks comment on various aspects of this definition. The Commission also notes that under the *CAN-SPAM Act*, whether an electronic mail message is considered “commercial” is based upon its “primary purpose,” and that a commercial message by definition does not include a transactional or relationship message.¹³

A. Transactional and Relationship Messages Require an Established Business Relationship

Unlike the national do-not-call list under the Telephone Consumer Protection Act,¹⁴ the *CAN-SPAM Act* does not contain an established business relationship exception. The *CAN-SPAM Act*, however, exempts from the definition of commercial messages those “transactional or relationship messages” that have one or more of several primary purposes.¹⁵

¹² *CAN-SPAM Act*, §14(d).

¹³ *Notice*, ¶ 11, *citing CAN-SPAM Act*, §3(2).

¹⁴ Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 104 Stat. 2394 (1991), *codified at* 47 U.S.C. § 227. The FCC adopted its portion of the National Do-Not-Call registry in Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, *Report and Order*, 18 FCC Rcd 14014, ¶ 28 (2003).

¹⁵ These include:

- (i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter with the sender;
- (ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;
- (iii) to provide—
 - 1. notification concerning a change in the terms or features of;
 - 2. notification of a change in the recipient’s standing or status with respect to; or
 - 3. at regular periodic intervals, account balance information or to other type of account statement with respect to,

Although the *CAN-SPAM Act* does not codify an “established business relationship” exception, the Commission should make clear that a party may not generate an SMS message that falls into the category of a transactional or relationship message unless it already does business with the recipient. To determine what is a “transaction or relationship” message, the Commission must consider the prior relationship between the sender and recipient. As the FCC found in the CPNI docket, consumers expect and desire businesses to use information accumulated in the provision of service to communicate with customers about other offerings.¹⁶ The FCC explained that “customers desire their service to be provided in a convenient manner, and are willing for carriers to use their CPNI without their approval to provide them service ... within the parameters of the customer-carrier relationship. Indeed, we agree with commenters that Congress recognized through sections 222(c)(1)(A) and (B) that customers expect that carriers with which they maintain an established relationship will use information derived through the course of that relationship to improve the customer's existing service.”¹⁷

-
- a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;
 - (iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or
 - (v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender. *CAN-SPAM Act*, Section 3(17)(A).

¹⁶ Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information; and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended, *Second Report and Order and Further Notice of Proposed Rulemaking*, 13 FCC Rcd 8061 (1998), ¶57.

¹⁷ *Id.*, ¶54. The FCC reaffirmed these findings in its most recent CPNI Order. See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’

The Commission should adopt a similar approach in implementing the *CAN-SPAM Act* because consumers likewise expect that businesses with which they are already doing business will communicate additional commercial opportunities in an effort to provide their customers with expanded service offerings. The express prior authorization requirement that applies to commercial messages does not apply to transactional and relationship messages for this same reason. When a consumer has a prior relationship with a company, it is more likely that he or she has voluntarily provided the company with the ability to send text messages to him or her and thus expects the communication in the course of doing business with the company.

As long as the primary purpose of a message falls within the broad parameters of Section 3(17)(A), the message should be not be considered a “commercial” message, even in the case where the message contains an advertisement or promotional component. The FTC is reviewing the meaning of these definitions in the context of its rulemaking to implement the *CAN-SPAM Act*, but the FCC must pursuant to Section 14(b) coordinate with the FTC on these matters as they relate to mobile messages. The FCC should adopt the FTC’s suggestion that a message should be considered commercial in nature when “an e-mail’s commercial advertisement or promotion is more important than all of the e-mail’s other purposes combined.”¹⁸

Use of Customer Proprietary Network Information and Other Consumer Information, *Third Report and Order and Third Further Notice of Proposed Rulemaking*, 17 FCC Rcd. 14860 (2002) (“CPNI Order”), ¶¶ 83-84.

¹⁸ Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act, 69 Fed. Reg. 11779 (proposed Mar. 11, 2004) (to be codified at 16 C.F.R. pt. 316).

B. Forwarded Messages Should Not Be Subject to the Restrictions That Apply to MSCMs

The Commission tentatively concludes that messages forwarded by a subscriber to his or her wireless device are not subject to the *CAN-SPAM Act*'s Section 14 requirements imposed on MSCMs.¹⁹ This conclusion is clearly correct.

The plain language of the statute defines MSCMs as those messages that are sent “directly” to a mobile device.²⁰ The legislative history of the *CAN-SPAM Act* makes very clear that “[s]pam sent to a desktop computer e-mail address, and which is then forwarded over a wireless network to a wireless device, i.e., delivered ‘indirectly’ from the initiator to the wireless device, would be treated by the rest of this bill and not by the additional Section 14 wireless-specific provisions we subject to an FCC rulemaking.”²¹ Indeed, in this case, it is the customer who is determining to forward these messages to the mobile device, and the customer can just as easily decide to stop forwarding the messages. Any other conclusion would be entirely unworkable because the protections including express prior authorization that relate only to MSCMs would then apply to all messages, not just those that are sent directly to a wireless device. This would be contrary to the statute, overbroad, and confusing.

III. THE COMMISSION SHOULD EXEMPT WIRELESS CARRIERS FROM THE REQUIREMENT TO SEEK EXPRESS PRIOR AUTHORIZATION

Congress recognized that wireless carriers are uniquely situated as providers of wireless service, and for this reason specifically directed the Commission to consider the relationship of wireless carriers to their customers when determining whether to subject

¹⁹ Notice, ¶ 12.

²⁰ *CAN-SPAM Act*, §14(d).

²¹ 149 Cong. Rec. H12854-02,12860 (daily ed. Dec. 8, 2003) (statement of Rep. Markey).

wireless carriers to the requirement to seek express prior authorization before sending MSCMs to their subscribers.²² If the Commission decides to exempt wireless carriers from this requirement, the Commission must adopt rules to require wireless providers to permit subscribers to indicate that they do not wish to receive future MSCMs from the provider: (1) at the time of subscribing to the service; and (2) in any billing mechanism.²³

The Commission should exempt wireless carriers from the requirement to seek express prior authorization before sending MSCMs to their customers as long as wireless carriers do not charge their customers for these messages. A requirement to seek such “opt-in” consent would raise a serious constitutional issue as to whether such a requirement would be an unlawful restriction on commercial speech. There is no reason to reach that issue because an exemption for wireless carriers to communicate with their own customers is warranted.

A. Wireless Carriers Are in a Unique Position With Their Subscribers

As the legislative history of the *CAN-SPAM Act* suggests, the FCC should “take into account the unique service and technical characteristics that may warrant wireless-specific rules affecting consumer and carrier rights and obligations.”²⁴ Indeed, the Commission has consistently recognized that wireless carriers warrant exemption from rules that otherwise limit contact with customers. For example, as noted above, the Commission’s rules exempt companies with established business relationships from the national do-not-call registry.²⁵ Also, in 1992 the Commission concluded that the TCPA

²² *CAN-SPAM Act*, §14(b)(3).

²³ *Id.*

²⁴ *Markey Statement* at H12195-6.

²⁵ Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, *Report and Order*, 18 FCC Rcd 14014, ¶ 42 (2003).

does not preclude wireless carriers from using autodialers and artificial or prerecorded voice messages to call their own subscribers as long as the subscribers are not charged for the calls.²⁶ And, as also referenced above, the FCC has recognized that allowing carriers to use CPNI obtained by virtue of the provision of service to a customer to market to the customer is permissible without consent.²⁷

Wireless carriers are the only entities that are in the position to suppress charges for MSCMs. As a result, wireless carriers have a special relationship with their customers, and this warrants exempting wireless carriers from the obligation to seek prior express authorization from their customers in order to send MSCMs. Verizon Wireless does not currently charge its customers for any SMS messages that Verizon Wireless originates, and Verizon Wireless would support a rule that required carriers to suppress charges in order to send MSCMs to their customers without receiving express prior authorization.

In addition, in some cases, the customer's access to service might depend on receiving such MSCMs. For instance, Verizon Wireless has no way to contact its pre-pay customers because it does not establish "reach" numbers with these customers. With only the number associated with the wireless pre-pay account, the best way for Verizon Wireless to contact these customers to inform them of important information, such as network outages, changes in service, and warnings regarding low balances, is via SMS messages.

²⁶ Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, *Report and Order*, 7 FCC Rcd 8752, ¶ 45 (1992).

²⁷ 47 C.F.R. § 64.2005(a).

B. Opt-In Consent is Disfavored Under The First Amendment

The Commission should also grant wireless carriers an exemption from seeking express prior authorization because such a requirement would be an unlawful restriction on commercial speech. As detailed above, Congress intended “express prior authorization” to require “opt-in” consent,²⁸ but the *CAN-SPAM Act* does not require the Commission to adopt an opt-in approach for wireless carriers to communicate with their customers.²⁹

As the Commission is aware, courts have disfavored opt-in consent requirements. In *U.S. West Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000) (“*U.S. West*”), the Tenth Circuit invalidated Commission rules that required opt-in approval for disclosures of CPNI outside the “total service” that a carrier offered to a customer, finding that the FCC had failed to provide the “empirical analysis and justification” necessary to support the opt-in regime’s restriction on speech. 182 F.3d at 1235. The Court found that the FCC had failed to give sufficient consideration to an approval mechanism such as an opt-out approach that was less restrictive on carriers’ speech. The Court held that the FCC could not “rely on its common sense judgment” on such issues, *id.* at 1239, but had to make a “careful calculation of the costs and benefits

²⁸ *Markey Statement* at H12195 (“The wireless spam provision of the bill offers wireless consumers relief by requiring an “opt-in” for spam to wireless consumers. This reflects the fact that spam to a mobile phone is more intrusive to consumers and the fact that some wireless payment plans currently charge users for the amount of text messages they receive.”)

²⁹ *Id.* (“Federal spam legislation ought to reflect the particular characteristics of wireless technology and use and this bill will allow the FCC to promulgate rules requiring a consumer “opt-in” for wireless email messages while examining the nature of a consumer’s relationship with their wireless phone and service to take into account the unique service and technical characteristics that may warrant *wireless-specific rules affecting consumer and carrier rights and obligations.*”) (emphasis added).

associated with the burden of speech imposed by its prohibitions.” *Id.* at 1238 (internal punctuation omitted). The Court held that the “FCC’s failure to adequately consider an obvious and substantially less restrictive alternative, an opt-out strategy, indicates that it did not narrowly tailor the CPNI regulations regarding customer approval.” *Id.* at 1238-39. The Court thus concluded that the FCC had not met its burden to show “that it had *narrowly tailored its regulations to meet its stated goal.*” *Id.* at 1239 (emphasis added).

More recently, the U.S. District Court for the Western District of Washington adopted the same approach as the court in *U.S. West* and permanently enjoined similar opt-in rules. *See Verizon Northwest, Inc. v. Showalter*, 282 F.Supp.2d 1187 (W.D. Wash. 2003) (“*Showalter*”). The Court held that the Washington Utilities and Transportation Commission (“WUTC”) had failed to meet its burden to show that the opt-in rules advanced the state’s asserted interest in consumer privacy “in a direct and material way.” *Id.* at 1193. More importantly, the Court held that the WUTC had failed to demonstrate that the opt-in rules were “narrowly tailored” to serve the state’s interests. *Id.* at 1195.

Both the federal scheme struck down in *U.S. West* and the Washington State regulations struck down in *Showalter* allowed carriers to use confidential information without subscriber consent to, among other things, market additional services to their own customers within the category of services that the customer already receives. *See U.S. West*, 182 F.3d at 1230 (“Broadly stated, the regulations permit a telecommunications carrier to use, disclose, or share CPNI for the purpose of marketing products within a category of service to customers, provided the customer already subscribes to that category of service”); *see also Showalter*, 282 F.Supp.2d at 1189 (“Use of private account information for ‘same-category marketing’ is not restricted”). In

contrast, a requirement to seek opt-in consent before sending messages to the carrier's own customers would burden substantially more speech than did the regulatory schemes struck down by the *U.S. West* and *Showalter* courts.

Before the Commission could impose an opt-in requirement on wireless carriers in this case, the Commission must at a minimum undertake an empirical analysis that *U.S. West* and *Showalter* make clear are required under the First Amendment to support serious restrictions on commercial speech. Even assuming privacy would represent a substantial state interest in the abstract, the Commission must demonstrate that the *specific restriction* directly advances a substantial state interest. *U.S. West*, 182 F.3d at 1235. There can be no argument that restricting carriers' ability to communicate with their customers invades consumers' privacy interests. On the contrary, as previously noted, the FCC has found in the CPNI context that consumers expect and want carriers to communicate with them to inform them of new offerings.

IV. THE COMMISSION SHOULD NOT CREATE A NATIONAL "DO-NOT-SMS" REGISTRY

The FCC seeks comment on whether to establish a do-not-SMS registry similar to the national do-not-call list.³⁰ Such a registry is not in the public interest.

Verizon Wireless opposes public access to lists of wireless numbers foremost because in the wrong hands such a list could result in abuse. Many wireless customers do not want to receive unexpected calls on their wireless phones. There are many reasons for this, including the fact that most wireless customers continue to pay for incoming calls, either on a per-minute basis or as a reduction of minutes. Creating a do-not-SMS

³⁰ Notice, ¶ 29. The Commission recognizes that the *CAN-SPAM Act* requires the FTC to create a plan to implement a do-not-email registry. *Id.* The *CAN-SPAM Act* does not require a similar do-not-SMS registry.

list, in attempting to solve one problem, would create a potentially worse one, revealing to anyone with a will to pay for such a list a registry of wireless numbers.

Today it is unlawful for any person to use an autodialer or artificial or prerecorded message to call a number assigned to a wireless service unless there is no charge for the call.³¹ To deal with this prohibition, the Direct Marketing Association (“DMA”) has for many years offered a “Wireless Suppression Service” that has assisted telemarketers in identifying wireless numbers. Given the advent of intermodal number portability, it has become much more complicated to discern whether a particular number is associated with a wireline or wireless service. To deal with this, NeuStar is developing a service that will keep track of ported numbers.³²

Verizon Wireless urges the Commission to require NeuStar and resellers of NeuStar’s database such as the DMA to protect this highly sensitive information. In the wrong hands, such information could foment spam because often the only information a spammer needs to send a message to a wireless handset is the wireless number. A national do-not-SMS list would create another opportunity for spammers intent on abuse to obtain wireless numbers.

V. THE FCC SHOULD AVOID MANDATING SPECIFIC TECHNICAL SOLUTIONS FOR PREVENTING SPAM

The *CAN-SPAM Act* requires the Commission to consider the ability of a sender of a commercial electronic mail message to reasonably determine that the message is an MSCM, and, consistent with that: (1) provide wireless subscribers the ability to avoid receiving MSCMs unless they have given express prior authorization, and (2) allow

³¹ 47 C.F.R. 64.1200(a)(1)(iii).

³² See NeuStar comments in CG Docket No. 02-278 (filed April 15, 2004).

recipients of MSCMs to indicate electronically a desire not to receive future MSCMs.³³ Senders of commercial e-mail should be able to discern whether a message is bound for a wireless handset from the domain name assigned to the service. For instance, messages sent to wirelessnumber@vtext.com are destined for a Verizon Wireless subscriber with the wireless number indicated in the address.

Given that the *CAN-SPAM Act* requires that customers have the ability to indicate electronically a desire not to receive MSCMs in the future after receiving them, the Commission proposes a variety of different methodologies to accomplish this, including personal identifiers, secret codes, and challenge-response mechanisms.³⁴ The Commission should not impose technical requirements on wireless carriers to implement these *CAN-SPAM Act* requirements.

As an initial matter, the duty to comply with the electronic disapproval requirement rests solely on the party sending the MSCMs. Wireless carriers have no control over these parties, making it impossible for wireless carriers to ensure their compliance. In addition, ordering a specific mechanism such as a challenge-response system, PINs, secret codes, and others will effectively preclude development of other more efficient remedies.³⁵ Technology vendors are working to build technologies that enable customers to control spam. Any specific mandated solution it might work now but not as networks evolve, it might work for some networks but others, or it might not work at all. The marketplace will develop technical solutions to control spam because

³³ *CAN-SPAM Act*, §§14(b)(1)-(2) & (d).

³⁴ *Notice*, ¶ 37.7

³⁵ For instance, the Commission in the E911 context ordered a network solution but the industry ultimately developed a more accurate handset solution.

companies have incentives to distinguish themselves and protect their customers against spam.

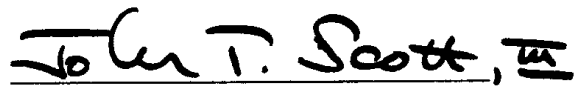
Rather than imposing specific technical standards to combat spam, the Commission should instead adopt broad guidelines for how electronic disapproval should work. For instance, the FCC could mandate that disapproval can be registered from the customer's handset or through the Internet. In this fashion, companies will have broad parameters around which to craft technical solutions.

CONCLUSION

For the foregoing reasons, the Commission should adopt measures to inhibit the growth of spam while maintaining carriers' right to communicate with their own customers.

Respectfully submitted,

VERIZON WIRELESS

A handwritten signature in black ink that reads "John T. Scott, III". The signature is written in a cursive, slightly stylized font. The "J" is large and loops around the "o". The "S" is also large and loops around the "c". The "III" is written as three distinct vertical strokes.

John T. Scott, III
Charon Phillips
1300 I St, N.W.
Suite 400 West
Washington, D.C. 20005
(202) 589-3740

April 30, 2004

Its Attorneys